

在RV34x系列路由器上配置基本防火墙设置

目标

本文的目的是说明如何在RV34x系列路由器上配置基本防火墙设置。

简介

防火墙的主要目标是通过分析数据包并基于预定规则集确定是否允许其通过来控制传入和传出网络流量。路由器被视为强大的硬件防火墙，因为其功能允许过滤入站数据。网络防火墙在假定为安全且受信任的内部网络与通常认为不安全且不受信任的外部网际网络（如Internet）之间建立桥接。

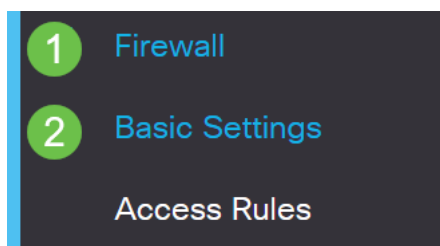
适用设备 | 固件版本

- RV34x系列 | 1.0.03.21 ([下载最新版本](#))

配置基本防火墙设置

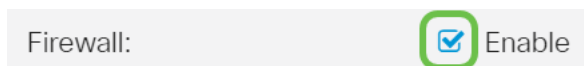
第 1 步

登录到Web用户界面(UI)，然后选择防火墙>基本设置。



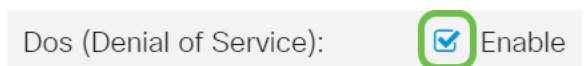
步骤 2

选中Enable Firewall复选框以激活Firewall功能。默认情况下启用该接口。



步骤 3

选中Enable Dos(Denial of Service)复选框以保护您的网络免受DoS攻击。默认情况下启用该接口。



步骤 4

选中**Enable Block WAN Request**复选框以拒绝对RV34x系列路由器的ping请求。默认情况下启用该接口。

Firewall:	<input checked="" type="checkbox"/> Enable
Dos (Denial of Service):	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable

步骤 5

在LAN/VPN Web Management区域中，选中**HTTP**和/或**HTTPS**复选框以启用来自这些协议的流量。在本例中，HTTPS复选框已选中。

- HTTP — 超文本传输协议是Internet上使用的数据传输协议。
- HTTPS — 超文本传输协议安全是HTTP的安全版本，可加密数据包以提高安全性。

LAN/VPN Web Management:	<input type="checkbox"/> HTTP	80	(Default: 80, Range: 1025 - 65535)
	<input checked="" type="checkbox"/> HTTPS	443	(Default: 443, Range: 1025 - 65535)

步骤 6 (可选)

选中**启用远程Web管理**复选框以启用远程管理。否则，请跳至步骤8。

通过选择单选按钮选择用于连接防火墙的协议类型。选项为**HTTP**和**HTTPS**。

输入允许远程管理的1025到65535之间的端口号。默认值为443。在本例中，使用1666。

Remote Web Management:	<input checked="" type="checkbox"/> Enable 1
	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS 2
3 Port	1666 (Default: 443, Range: 1025 - 65535)

步骤 7

在Allowed Remote IP Addresses区域中，选择单选按钮以允许任何IP地址远程访问网络或指定IPv4或IPv6地址范围。在本例中，选择了IP范围。在本例中，起始IP地址为128.112.59.21，结束IP地址为128.112.59.34。

Allowed Remote IP Addresses:	<input type="radio"/> Any IP Address
<input checked="" type="radio"/>	128.112.59.21 to 128.112.59.34 (IPv4 or IPv6 address range)

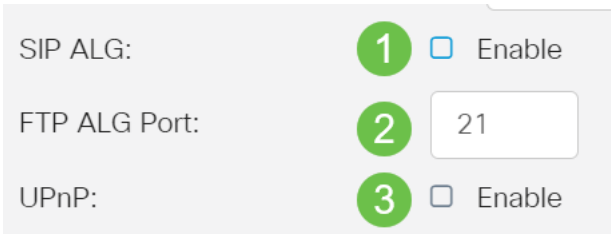
步骤 8 (可选)

选中**Enable SIP ALG**复选框以启用会话初始协议(SIP)应用层网关(ALG)以通过防火墙。可启用此功能，以帮助SIP数据包通过防火墙。SIP数据包用于发起语音流量的连接。如果您的VoIP提供商使用不同的网络地址转换(NAT)遍历协议，则可禁用此功能 (默认设置)。

在FTP ALG Port字段中指定SIP ALG的文件传输协议(FTP)端口。默认值为 21。

选中**Enable UPnP**复选框以启用通用即插即用(UPnP)。默认情况下禁用此功能。

在本例中，这些选项保持禁用状态。



SIP ALG: Enable (1)

FTP ALG Port: (2)

UPnP: Enable (3)

步骤 9 (可选)

在Restrict Web Feature (限制Web功能) 区域下，选中Block (阻止) 区域中要阻止的Web功能类型的复选框。默认情况下，这些复选框处于禁用状态。选项有：

Java — 将阻止包含此类Web元素的所有Web元素。此设置有助于防止基于Java的Web攻击。

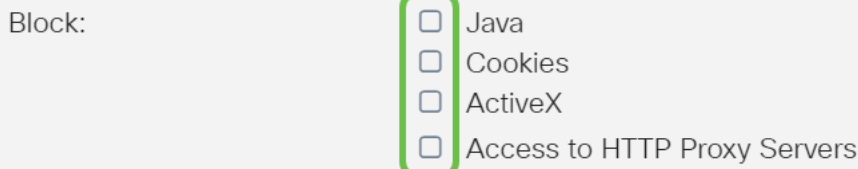
Cookie - Cookie是存储在计算机中的数据，用于帮助网站了解访问它们的人员。阻止他们可以阻止恶意Cookie访问数据。

ActiveX — 它是Microsoft开发的一个插件，用于改善浏览体验。阻止它可防止恶意ActiveX插件危害网络设备。

对代理HTTP服务器的访问 — HTTP代理服务器隐藏最终用户的详细信息，使其免受黑客攻击。他们是中间人，因此客户不直接访问Internet。但是，如果本地用户能够访问WAN代理服务器，他们可能会找到绕过路由器内容过滤器的方法来访问路由器阻止的互联网站点。

在本例中，复选框保持禁用状态。

Restrict Web Features



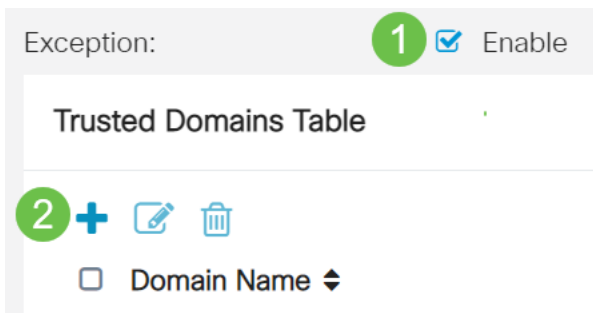
Block:

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

步骤 11 (可选)

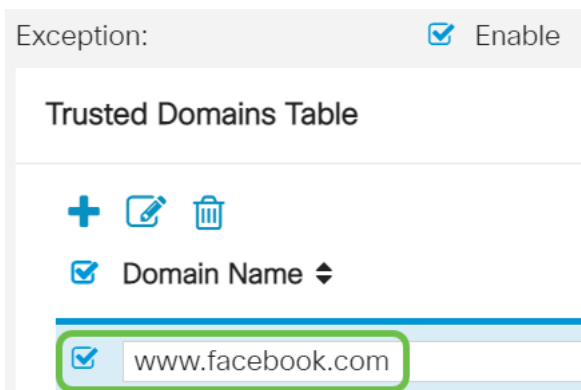
选中**Enable Exception**复选框，以仅允许选定的Web功能 (如Java、Cookie、ActiveX或HTTP代理服务器访问) 并限制所有其他功能。默认情况下它是禁用的。在本例中，它处于禁用状态。

在受信任域表中，单击**添加图标**以添加受信任或允许访问网络的域。



步骤 12

在域名字段中，输入要授予对网络访问权限的域名。在本例中，[使用 www.facebook.com](#)。



步骤 13

单击 Apply。



步骤 14 (可选)

要永久保存配置，请转至“复制/保存配置”页，或单击页面上部的保存图标。



结论

现在，您应该已在RV34x系列路由器上成功配置基本防火墙设置。